



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT APPLICATION OF

PUHAKAINEN, Pekka

Group Art Unit:2666

RECEIVED

NOV 10 2004

Appln. No.: 09/555,236

Examiner: Harper, Kevin E. Technology Center 2600

Filed: May 25, 2000

TITLE: METHOD AND EQUIPMENT FOR IDENTIFYING A LOGICAL CHANNEL

* * * * *

DECLARATION UNDER RULE 131

Hon. Commissioner of Patents
and Trademarks
Washington, D.C. 20231

Sir:

I, Mr. Kari Ahokas, declare as follows:

1. I am the Patent Engineer at Nokia Networks Oy who has been and continues to be responsible for preparation, filing and prosecution of the above-identified application, U.S. Patent Application Serial No. 09/555,236 and its priority application, FI 974381.
2. A photocopy of a Nokia Invention Report is attached at Appendix A (see also its certified English language translation attached at Appendix B) This Invention Report was signed by me on November 27, 1996, following its submission to me by the named inventors for the above-identified application. This Invention Report evidences the inventors' conception of the method and equipment for identifying a logical channel described in the Report.
3. A decision was made by Nokia Networks Oy to file for patent protection for the technology disclosed in the Invention Report. That decision was made December 13, 1996.
4. Drafting of a patent application to cover the technology disclosed in the Invention Report in Finland began on September 1, 1997.

5. A preliminary draft of the Finnish patent application was sent to the named inventors and myself on November 17, 1997.
6. A final draft of the Finnish patent application was sent to the named inventors and myself on November 27, 1997.
7. The Finnish patent application, FI 974381, was filed in the Finnish Patent Office on December 1, 1997.
8. I hereby acknowledge that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. § 1001) and may jeopardize the validity of the present application or any patent issuing thereon. All statements made of my own knowledge are true and all statements made on information and belief are believed to be true.

By: Kari Ahokas
Mr. Kari Ahokas

Date: October 8, 2004

APPENDIX A

INVENTION REPORT

Title of the invention

Method and apparatus for verifying a logical channel [handwritten text]
(Reliable stealing identifier for a TETRA receiver)

Inventor(s)

Pekka Puhakainen and Timo Viero

BRIEF DESCRIPTION OF THE INVENTION

1. OBJECT OF THE INVENTION

- To what does the invention relate? A method, device, system etc.?
- For what is the method or device of the invention employed?

The invention relates to a method of identifying stealing in a TETRA receiver.

The TETRA standard permits the stealing of traffic capacity when an STCH message or messages are transmitted on a traffic channel. The existence of stealing, i.e. STCH is indicated to the receiver by replacing the normal training sequence 1 with a normal training sequence 2.

In the GSM standard... [handwritten text]

2. PROBLEM

- Which problem does the invention solve?

In empirical measurements with a prototype of a base station, we have observed that indicating stealing by changing training sequences is quite an insecure method. Under normal circumstances, the channel is fading and contains noise, whereby a TETRA receiver (its synchronization block) erroneously interprets a normal training sequence 1 as a normal training sequence 2, which again makes the receiver erroneously conclude that stealing is concerned, and thereby the data transfer capacity of the traffic channel (TCH/S, TCH/7.2, TCH/4.8 and TCH/2.4) is reduced. Naturally, the receiver may erroneously interpret a transmitted normal training sequence 2 as a normal training sequence 1, whereby a transmitted STCH message or messages are lost, since they are erroneously interpreted as normal data of the traffic channel. Our invention is also usable for eliminating such situations.

Normal training sequences 1 & 2 only contain 22 bits, and thus reliable distinguishing a normal training sequence 1 from a normal training sequence 2 under noisy and fading circumstances is extremely difficult, if not impossible. The problem is more serious in a base station than in a mobile, since in a base station a training sequence transmitted by a mo-



bile has to be searched for in a long "time window" because of the movement of the mobile. With the present DSP software in the TU50 channel model, 0.8% of received messages are erroneously interpreted as stolen at a sensitivity limit. The problem also appears in a static (AWGN) channel and therefore e.g. the TCH/S (speech) channel does not fulfil the requirements of the conformance test of a static channel. Generally, it can be stated that erroneously interpreted stealings cause the most problems in channels comprising efficient channel coding, wherein the bit-error-ratio should be extremely low.

3. KNOWN SOLUTIONS

- How has the problem been solved previously?
- What are the drawbacks of known methods or devices?

We are only aware of a solution suggested by a standard, wherein stealing is identified in the training sequence. As mentioned above, this method is sensitive to noise.

4. THE INVENTION

- What is the basic idea of the invention?
- Crystallize the invention using one sentence.
- What is new and inventive in the invention?
- English-language search words for patent searches.

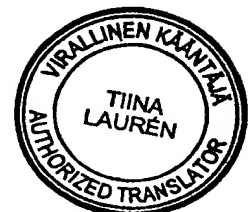
The idea of our invention is to utilize channel decoding when concluding if stealing actually has occurred in the case of a normal training sequence 2.

In our invention, we utilize the functional blocks of a TETRA receiver in an exceptional manner, such as channel decoding, and are thus able to improve the quality of a connection over the air interface.

5. ADVANTAGES OF THE INVENTION

- How does the invention eliminate or sidestep the drawbacks of known solutions?
- What other advantages does the method or device according to the invention possess?
- Are any drawbacks associated with the invention? Which are they?

The invention ensures that a NOKIA TETRA base station receiver (and vehicle station & hand radio) fulfils the requirements of the conformance test using normal DSP software. If the invention is not employed, we have to change the normal DSP software for instance by not allowing stealings in the conformance test. We are thus of the opinion that without our invention, the NOKIA TETRA system does not seem to fulfil the requirements of the conformance test. Because of future improvements of the synchronization algorithm, we leave a slight reservation in our conclusion.



The invention improves the performance of a receiver in a normal operational mode. Speech quality improves, since our invention eliminates unnecessary stealings in speech channels. Circuit-switched data channels also operate without interrupting 'pseudo stealings'.

The drawback of the invention is increased need for DSP computation, which causes a delay in decoding messages. This delay will be about 0.2 to 0.6 ms, i.e. tolerable.

6. OPERATION OF THE INVENTION

- Detailed description of at least one embodiment or implementation with the use of flow charts, block diagrams, signalling diagrams and other figures illustrative of the operation of the invention

In the following, we will describe how we use channel decoding for ascertaining that stealing (STCH) is involved. The enclosed logics are combined with the FRAME task (BS) and the SIGNALLING process (MS), wherein channel decoding takes place at the present moment, too.

TOOLS OF OUR INVENTION FROM THE CHANNEL DECODING LIBRARY:

The enclosed message decoding methods, included in TETRA, are at our disposal.

Decoding an STCH message, particularly its CRC computation. The probability that CRC does not detect that a STCH message is erroneously decoded is in the order of 0.00001.

Decoding a TCH/S message, particularly CRC computation of Class 2 bits. The probability that CRC does not detect that Class 2 bits are erroneously decoded is in the order of 0.004.

Decoding a TCH/S (when STCH in the first slot half) message, particularly CRC computation of Class 2 bits. The probability that CRC does not detect that Class 2 bits are erroneously decoded is in the order of 0.06.

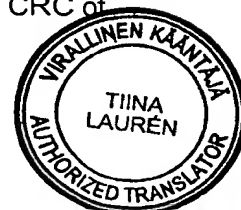
Accordingly, we are able to conclude that the CRC of an STCH message is extremely reliable as compared with the reliability of the CRC of TCH/S channels. TCH/S CRC computation is so unreliable that we will not use them at all. This reduces the DSP processing delay caused by the invention.

ALGORITHM FOR RELIABLE IDENTIFICATION OF STEALING ON TCH/S, TCH/7.2, TCH/4.8 AND TCH/2.4 CHANNELS

Once a normal training sequence 2 is detected, then

1) Decode the first half slot as an STCH. If CRC is OK then believe that stealing really has taken place. In other words, the training sequence is maintained as a normal training sequence 2, and the decoding of the message/burst is continued as usual.

2) If the CRC of the STCH of the first half slot indicates a decoding error for STCH, then an attempt is made to decode half slot 2 as an STCH. If the CRC of



the second STCH is OK, then we conclude that stealing (STCH + STCH) is involved. Accordingly, the normal training sequence 2 is maintained. If the CRC of the STCH of the second half also indicates a decoding error, then we interpret that no stealing has taken place in the received slot; instead, TCH data is involved. Accordingly, the algorithm replaces the normal training sequence 2 with a normal training sequence 1.

A comment on the algorithm:

Even if stealing were involved when we replace the normal training sequence 2 with a normal training sequence 1, then, however, said STCH messages could not be decoded correctly, wherefore our algorithm does in no way weaken the signalling capability by means of stealing. If the wrong interpretation of a normal training sequence 1 as a normal training sequence 2 was involved, then our algorithm has successfully saved one TCH message, e.g. a speech message, from being destroyed. If stealing (STCH) actually was involved, which channel decoding is no longer able to decode, then we erroneously interpret the STCH message as a TCH message, which causes bit errors in the TCH data. Speech CRC computation is able to identify erroneous decoding and prevent the entry of an erroneous message into a speech codec. The effect of the error made by our algorithm on TCH/7.2, TCH/4.8 and TCH/2.4 channels is difficult to estimate accurately, since we are not aware of the application employing these channels.

7. ALTERNATIVE IMPLEMENTATIONS

- What other embodiments or implementations does the invention have?
- Which embodiment or implementation can be considered the best? Why?

8. BECOMING PUBLIC OF THE INVENTION

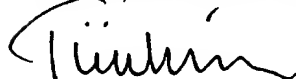
- Is the invention already employed or will it be employed or made public soon? When? Where?

9. REFERENCES

- Information about published patents, standards etc. relating to the matter
- Differences of the invention as compared with inventions disclosed in the published patents

I hereby certify the above to be a true and correct translation of the attached document.

Helsinki, 07 October 2004



Tiina Laurén
Authorized Translator (Act 1148/88)



APPENDIX B

LUOTTAMUKSELLINEN

☐ Arkistokappale A
☐ Keksijän kappale B

Lausuntokappale KOPIO hyväksytty / 19
Ilmoitus keksijälle KOPIO hyväksytty / 19

KEKSINTÖILMOITUS

Keksinnön nimi

Luotettava varastuksen tunnistin
TETRA vastaanottimeen

Keksijä (!), arvo tai ammatti

*51121
Pekka Puhakainen, tutkimusinsinööri
Timo Viero, tutkimusinsinööri

Kotiosoite

Oskari 1C 28, 02150 Espoo

Isomäkeläsaarentie 3 G 64, 00560 Helsinki

Keksinnön lyhyt kuvaus

Kats. liite.

Keksintö kuuluu A ryhmään*)
(Voidaan jättää täyttämättä)

Liitteitä 1 kpl

Keksintö (Tuote) julkaistaan 1 4 1997

Ilmoitan/Ilmoitamme täten, että katson/katsomme keksinnön kuuluvan ylle merkitsemään/merkitsemäämme ryhmään ja että tietääkseni/tietääksemme olen/olemme ainoa(!) ja oikeat(!) keksijät(!).

Yhtiö saattaa voimassa olevan lain perusteella olla oikeutettu saamaan kokonaan tai osittain oikeuden keksintöön. Sitoudun/Sitoudumme allekirjoittamaan keksijänä/keksijöinä kaikki ne asiakirjat, jotka voidaan tarvita keksinnön suojaamiseen eri maissa.

Keksijän/Keksijöiden allekirjoitukset

Aika 25 11 1996

Allekirjoitus

Timo Viero Pekka Puhakainen

5

OLEN SAANUT TIEDON YHTIÖN PÄÄTÖKSESTÄ KOSKIEN YLLÄ MAINITTUA KEKSINTÖÄ

Keksijän/Keksijöiden allekirjoitukset

Aika 1 19

Allekirjoitus

KEKSINTÖILMOITUS VASTAANOTETTU

Koodi NC 10860 Yhtiö NTC Osasto PMR

Paikka Espoo Aika 27.11.1996

Allekirjoitus *Kari Ahola*

3

KEKSINNÖN ARVIOINTI

(Kyllä = 1, ehkä = 2, ei = 3)

Teknisesti

☐ uusi
☐ toteutettavissa
☐ patentoitavissa

Kehitysmielessä

☐ valmis suojattavaksi
☐ kehitystyötä jatketaan
☐ kehityskelpoinen idea

Markkinoinnin kannalta

☐ hyvin arvokas
☐ myyntivaltti
☐ kannattaa patentoida

Käyttöoikeuden kannalta

☐ tärkeä suojata
☐ helppo valvoa
☐ vaikea kiertää

Keksintö kuuluu mielestäni _____ ryhmään*)

Ehdotan, että ilmoitettu keksintö

☐ varataan yhtiön käyttöön
☐ jätetään keksijän käyttöön

Paikka Aika

Allekirjoitus

4

ILMOITUS KEKSIJÄLLE

Ilmoitan, että yhtiö on tämän keksintöilmoituksen huolellisesti tutkittuun päättänyt

☐ varata keksinnön itselleen
☐ varata keksinnön käyttöoikeuden itselleen
☐ antaa keksijälle vapauden itsenäiseen menettelyyn
☐ antaa ilmoituksen oheisella liitteellä

☐ salata keksinnön
☐ hakea keksinnölle patenttia
☐ olla hekematta keksinnölle patenttia
☐ päättää vasta myöhemmin patentin hausta
Keksintö kuuluu ryhmään _____

Tähän päätökseen tyytymätön keksijä voi hakea muutosta valittamalla 30 vrk kuljessa yhtiön hallitukselle.

Ilmoituspaikkio

Paikka Aika

Allekirjoitus

KEKSINTÖILMOITUS

Keksinnön nimi

Menetelmä ja laitteisto loogisen kanavan varmistamiseksi
(Luotettava varastuksen tunnistin TETRA vastaanottiin)

Keksijä(t)

Pekka Puhakainen ja Timo Viero

KEKSINNÖN LYHYT KUVAUS

1 KEKSINNÖN KOHDE

- Mitä keksintö koskee? Menetelmää, laitetta, järjestelmää, jne?
- Mihin keksinnön mukaista menetelmää tai laitetta käytetään?

Keksintö koskee menetelmää varastuksen tunnistamiseksi TETRA-vastaanottimessa.

TETRA standardissa sallitaan varastus liikennöintikapasiteetista jolloin liikennekanavalla lähetetään STCH viesti tai viestejä. Varastuksen eli STCH:n olemassaolo osoitetaan vastaanottimelle vaihtamalla normal training sequence 1 normal training sequence 2:ksi.

GSM-standardissa

2 ONGELMA

- Minkä ongelman keksintö ratkaisee?

Käytännön mittauksissa tukiaseman prototyyppillä olemme havainneet että varastuksen indikointi opetusjaksoa muuttamalla on varsin epävarma menetelmä. Normaleissa toimintaolosuhteissa kanava on häipyvä ja sisältää kohinaa jolloin TETRA vastaanotin (sen synkronoimislohko) virheellisesti erehtyy tulkitsemaan normal training sequence 1:n normal training sequence 2:na mikä taas saa vastaanottimen virheellisesti päättelemään että varastus on kyseessä ja täten liikennöintikanavan (TCH/S, TCH/7.2, TCH/4.8 sekä TCH/2.4) tiedonsiirtokapasiteetti laskee. Vastaanotin voi luonnollisesti erehtyä luulemaan lähetettyä normal training sequence 2:sta normal training sequence 1:ksi jolloin lähetetty STCH viesti tai viestit menetetään koska ne tulkitaan virheellisesti liikennekanavan normaaliaksi dataksi. Keksintöämme voidaan käyttää myös näiden tilanteiden poistamiseen.

Normal training sequence 1 & 2 sisältävät vain 22 bittiä joten normal training sequence 1:n erottaminen varmasti normal training sequence 2:sta kohinaisissa ja häipyvissä olosuhteissa on erittäin vaikeaa ellei mahdotonta. Ongelma on mobiilia suurempi tukiasemassa jossa mobiiliin lähettämää opetusjaksoa joudutaan etsimään pitkistä "aikaikkunasta" mobiiliin liikkeen takia. Nykyisellä DSP ohjelmistolla TU50 kanavamallissa 0,8% vastaanotetuista viesteistä tulkitaan virheellisesti varastetuiksi herkkyysrajalla. Ongelma ilmenee myös staattisessa (AWGN) kanavassa ja sen johdosta esimerkiksi TCH/S (puhe) kanava ei täytä conformance testin staattisen kanavan vaatimuksia. Yleisesti voidaan todeta että väärin tulkitut varastukset aiheuttavat eniten ongelmia tehokkaan kanavakoodauksen sisältäville kanaville joissa bittivirhesuhteen pitäisi olla erittäin pieni.

3 TUNNETUT RATKAISUT

- Miten ongelma on ratkaistu aikaisemmin?
- Mitkä ovat tunnettujen menetelmien tai laitteiden epäkohdat?

Tiedossamme on vain standardin ehdottama ratkaisu, jossa varastus tunnistetaan opetusjaksosta. Kuten kerroimme yllä tämä menetelmä on kohinaherkkä.

4 KEKSINTÖ

- Mikä on keksinnön perusidea?
- Keksinnön kiteytys yhdellä lauseella.
- Mikä keksinnössä on uutta ja omalaatuista?
- Englanninkieliset hakusanat patenttihakuja varten.

Keksintömme ideana on käyttää hyväksi kanavadekoodausta pääteltäessä onko todellakin tapahtunut varastus normal training sequence 2:n tapauksessa.

Keksinnössämme käytämme hyväksi poikkeuksellisella tavalla TETRA-vastaanottimen toiminnallisia lohkoja kuten kanavadekoodausta ja pystymme siten parantamaan yhteyden laatua yli ilmarajapinnan.

5 KEKSINNÖN EDUT

- Millä tavoin keksintö poistaa tai kiertää tunnettujen ratkaisujen epäkohdat?
- Mitä muita etuja keksinnön mukaisella menetelmällä tai laitteella on?
- Liittyykö keksintöön haittoja? Mitä?

Keksintö varmentaa sen että NOKIA TETRA tukiasemavastaanotin (ja ajoneuvoasema & käsiradio) täyttää conformance testin vaatimukset normaalilla DSP-ohjelmistolla. Jos keksintöä ei käytetä joudumme muuttamaan normaalia DSP ohjelmistoa esimerkiksi siten että varastuksia ei sallita conformance testissä. Mielestämme voimme siis sanoa että ilman keksintöämme NOKIA TETRA järjestelmä ei näytä täyttävän conformance testin vaatimuksia. Jätämme pienen varauksen päätelmäämme synkronointialgoritmin tulevien parannusten johdosta.

Keksintö parantaa vastaanottimen suorituskykyä normaalissa toimintamoodissa. Puheen laatu paranee kun keksintömme eliminoi turhat varastukset puhekanavista. Myös piiriytketyt datakanavat toimivat ilman keskeyttäviä "pseudovarastuksia".

Keksinnön haittana on lisääntynyt DSP laskentatarve joka aiheuttaa viivettä viestien dekodakseen. Tämä viive tulee olemaan noin 0.2-0.6 ms eli siedettävä.

6 KEKSINNÖN TOIMINTA

- Ainakin yhden sovellusmuodon tai toteutustavan seikkaperäinen selostus käyttäen apuna vuokaavioita, lohkoavioita, signaalointikaavioita tai muita keksinnön toimintaa valaisevia kuvia.

Seuraavaksi esitämme miten käytämme kanavadekoodausta varmentamaan onko kyseessä varastus (STCH). Oheinen logiikka yhdistetään FRAME-taskiin (BS) ja SIGNALLOINTI-prosessiin (MS) missä kanavadekoodaus nykyisinkin suoritetaan.

KEKSINTÖMME TYÖKALUT KANAVADEKODAAUSKIRJASTOSTA:

Käytössämme on oheisia TETRAan kuuluvia viestien dekodausmenetelmiä.

STCH sanoman dekodaus, erityisesti sen CRC laskenta. Todennäköisyys että CRC ei havaitse että STCH viesti on virheellisesti dekodattu on luokkaa 0,00001.
TCH/S sanoman dekodaus, erityisesti Class 2 bittien CRC laskenta. Todennäköisyys että CRC ei havaitse että Class 2 bitit on virheellisesti dekodattu on luokkaa 0.004.
TCH/S (kun STCH ensimmäisessä slotin puolikkaassa) sanoman dekodaus, erityisesti Class 2 bittien CRC laskenta. Todennäköisyys että CRC ei havaitse että Class 2 bitit on virheellisesti dekodattu on luokkaa 0.06.

Voimme siis päätellä että STCH viestin CRC on erittäin luotettava TCH/S kanavien CRC:n luotettavuuteen verrattuna. TCH/S CRC-laskenta on niin epäluotettava että emme tule käyttämään niitä lainkaan. Tämä vähentää osaltaan keksintömme aiheuttamaa DSP prosessointiviivettä.

ALGORITMI LUOTETTAVAAN VARASTUKSEN TUNNISTUKSEEN TCH/S, TCH/7.2, TCH/4.8 JA TCH/2.4 KANAVILLA

Kun on havaittu normal training sequence 2 niin

1) Dekoodaa ensimmäinen half slot STCH:na. Jos CRC on OK niin uskotaan että varastus on todella tapahtunut. Eli opetusjakso säilytetään normal training sequence 2:na ja jatketaan viestin/purskeen dekodausta normaalisti.

2) Jos ensimmäisen half slotin STCH:n CRC osoittaa dekodausvirheen STCH:lle, niin yritetään dekodata half slot 2 STCH:na. Jos toisen STCH:n CRC on OK niin päättelemme että kyseessä on varastus (STCH + STCH). Normal training sequence 2 siis säilytetään. Jos toisenkin puoliskun STCH:n CRC ilmoittaa dekodausvirheestä niin tulkitsemme että vastaanotetussa slotissa ei ole tapahtunut varastusta vaan kyseessä on TCH dataa. Algoritmi vaihtaa siis normal training sequence 2:n 1:ksi.

Algoritmistä voidaan mainita seuraavaa:

Vaikka kyseessä olisikin varastus kun vaihdamme normal training sequence 2:n 1:ksi niin kyseisiä STCH-viestejä ei saataisi kuitenkaan dekodattua oikein joten signaalintykyä varastuksen avulla algoritmimme ei heikennä lainkaan. Jos kyseessä todella oli normal training sequence 1:n väärä tulkinta normal training sequence 2:na niin algoritmimme on onnistuneesti pelastanut yhden TCH viestin, esimerkiksi puheviestin, tuhoamisen. Jos kyseessä todella oli varastus (STCH) jota kanavadekoodaus ei enää kykene dekodamaan niin tulkitsemme STCH viestin virheellisesti TCH viestinä mikä aiheuttaa bittivirheitä TCH dataan. Puheen CRC laskenta voi tunnistaa virheellisen dekodauksen ja estää virheellisen viestin pääsyn puhekoodekkiin. TCH/7.2, TCH/4.8 ja TCH/2.4 kanavilla algoritmimme tekemän virheen vaikutusta on vaikea tarkasti arvioida koska emme tunne näitä kanavia käyttävää sovellutusta.

7 TOTEUTUSVAIHTOEHDOT

- Mitä muita sovellusmuotoja tai toteutustapoja keksinnöllä on?
- Mitä sovellusmuotoa tai toteutustapaa voidaan pitää parhaana? Miksi?

8 KEKSINNÖN JULKISEKSI TULO

- Onko keksintö jo käytössä tai tullaanko sitä pian käyttämään tai julkistamaan? Milloin? Missä?

9 VIITETIEDOT

- Tiedot asiaan liittyvistä patenttijulkaisuista, standardeista ym.
- Keksinnön erot verrattuna patenttijulkaisuissa kuvattuihin keksintöihin.